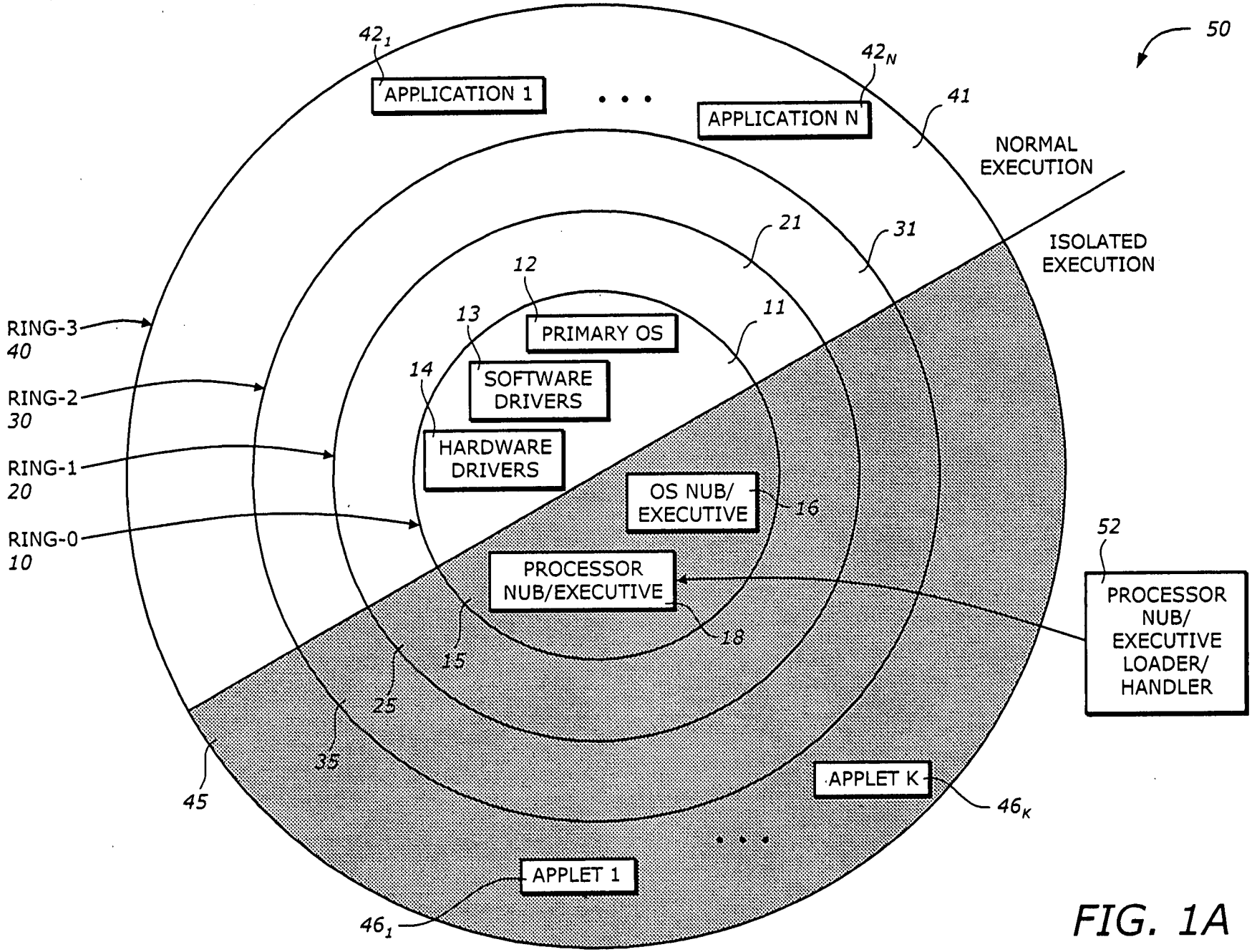


FIG. 1A

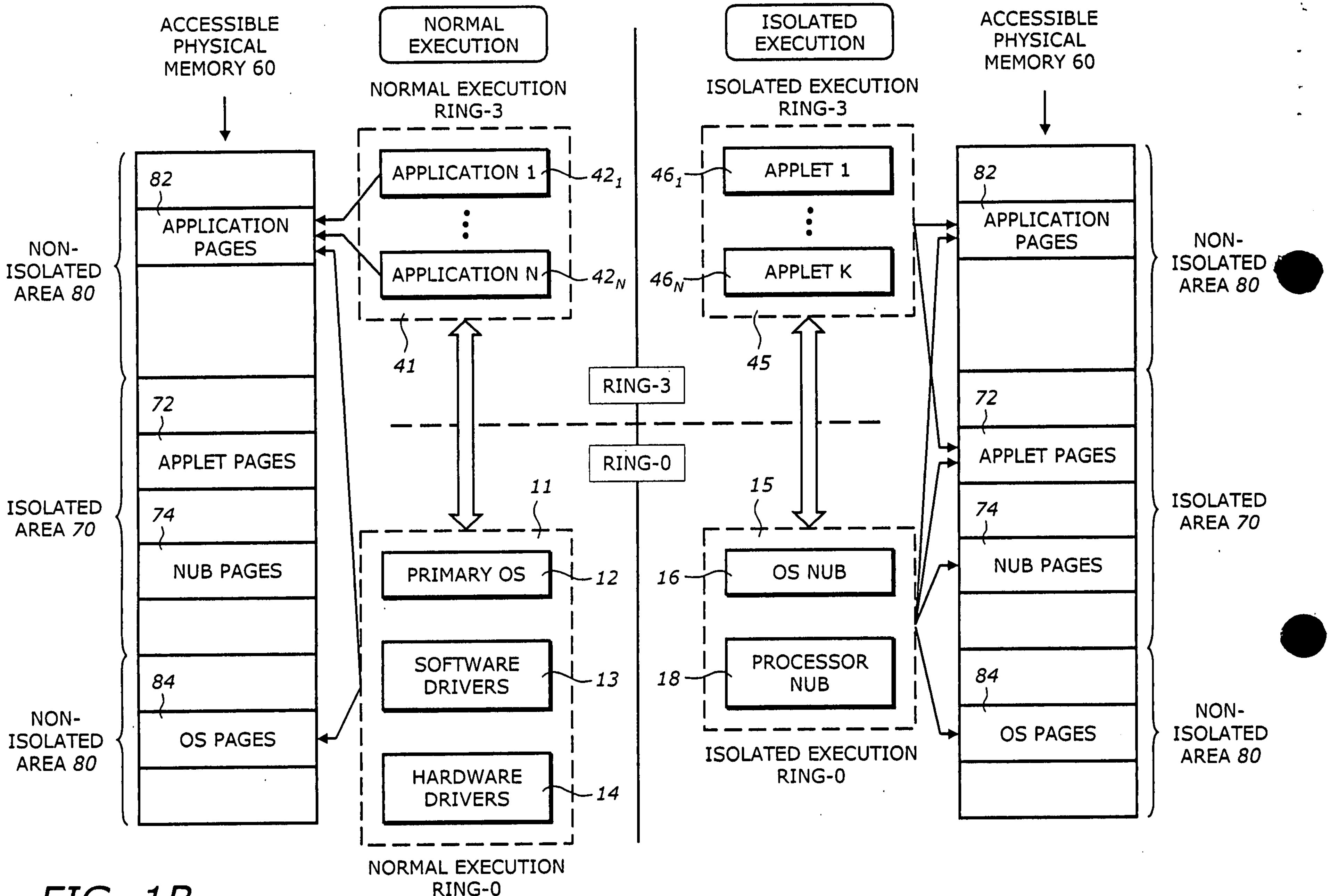
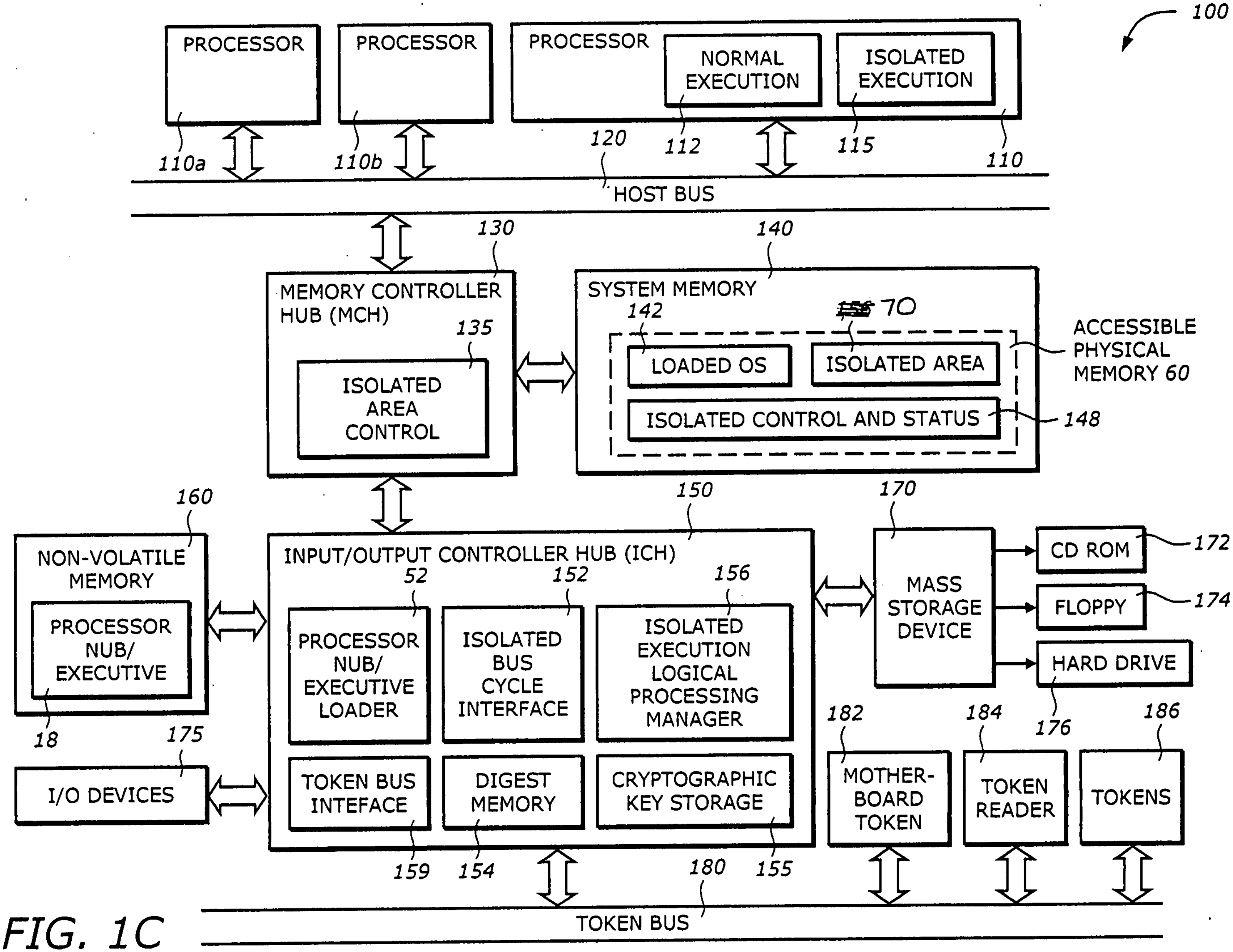

ACCESSIBLE PHYSICAL MEMORY 60
NORMAL EXECUTION
NORMAL EXECUTION RING-3
ISOLATED EXECUTION
ISOLATED EXECUTION RING-3
ACCESSIBLE PHYSICAL MEMORY 60
82
APPLICATION PAGES
NON-ISOLATED AREA 80
APPLICATION 1
42_1
APPLICATION N
42_N
41
46_1
APPLET 1
46_N
APPLET K
45
72
APPLET PAGES
ISOLATED AREA 70
74
NUB PAGES
RING-3
RING-0
11
PRIMARY OS
12
SOFTWARE DRIVERS
13
HARDWARE DRIVERS
14
15
16
OS NUB
18
PROCESSOR NUB
84
OS PAGES
NORMAL EXECUTION RING-0
ISOLATED EXECUTION RING-0

FIG. 1B



100
PROCESSOR
110a
PROCESSOR
110b
PROCESSOR
NORMAL EXECUTION
ISOLATED EXECUTION
120
112
115
110
HOST BUS
130
140
MEMORY CONTROLLER HUB (MCH)
135
ISOLATED AREA CONTROL
SYSTEM MEMORY
142
70
LOADED OS
ISOLATED AREA
ACCESSIBLE PHYSICAL MEMORY 60
ISOLATED CONTROL AND STATUS
148
160
150
170
NON-VOLATILE MEMORY
PROCESSOR NUB/ EXECUTIVE
18
INPUT/OUTPUT CONTROLLER HUB (ICH)
52
152
156
PROCESSOR NUB/ EXECUTIVE LOADER
ISOLATED BUS CYCLE INTERFACE
ISOLATED EXECUTION LOGICAL PROCESSING MANAGER
MASS STORAGE DEVICE
CD ROM
172
FLOPPY
174
HARD DRIVE
176
175
I/O DEVICES
TOKEN BUS INTEFACE
DIGEST MEMORY
CRYPTOGRAPHIC KEY STORAGE
182
184
186
MOTHER-BOARD TOKEN
TOKEN READER
TOKENS
159
154
180
155
TOKEN BUS

FIG. 1C

42390.P8107

00TEE0"4S68ES60

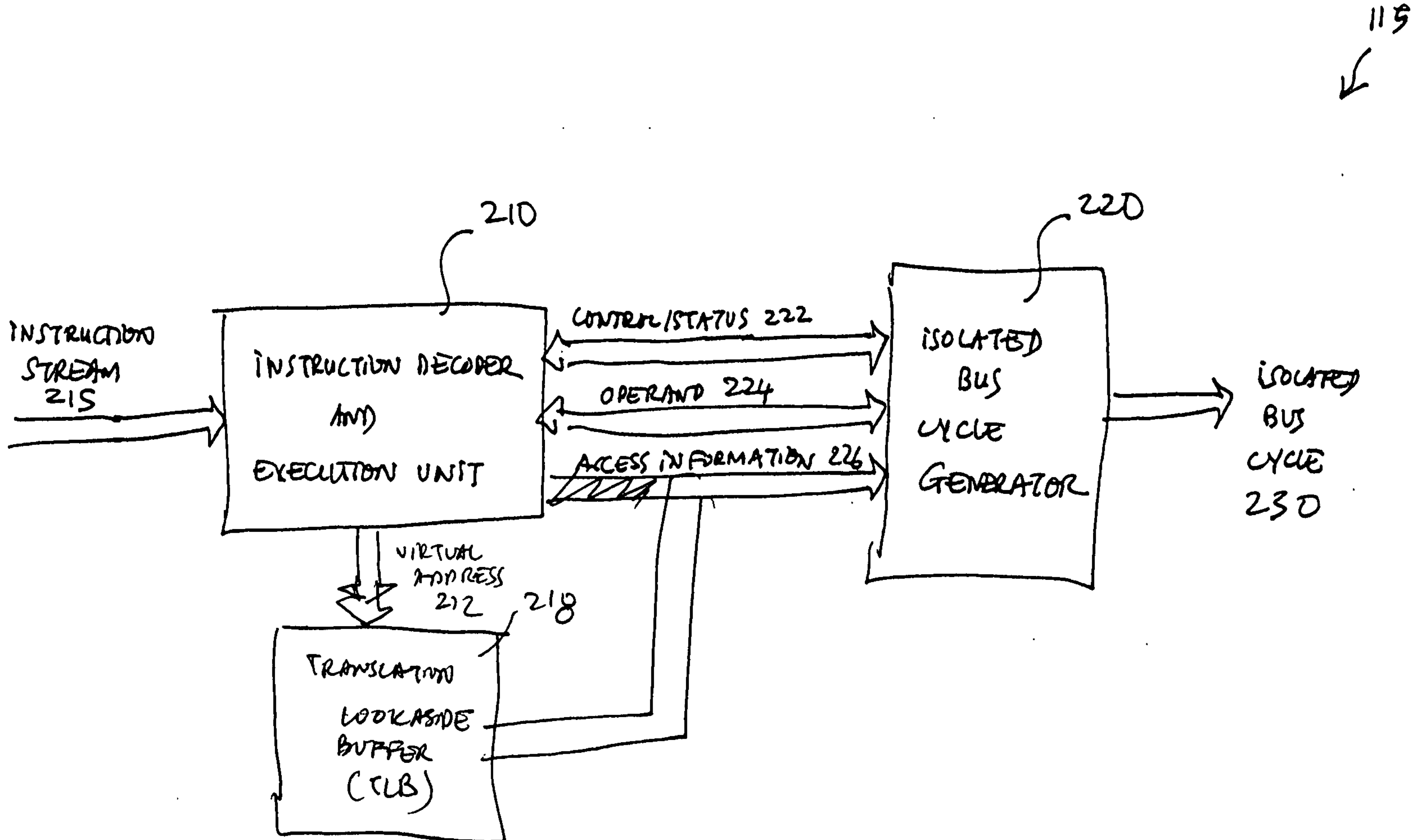


FIG. 2A

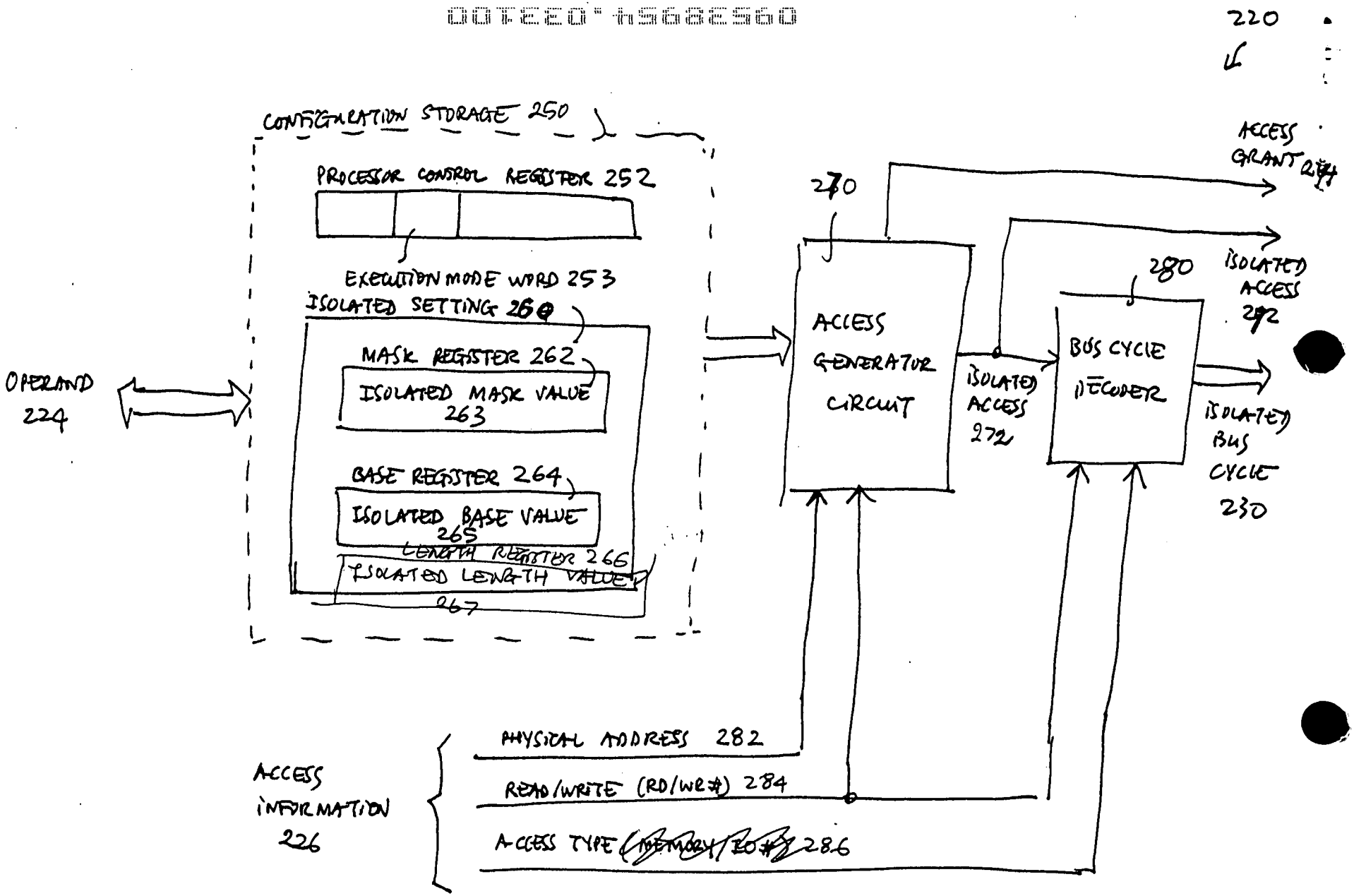

220
CONFIGURATION STORAGE 250
PROCESSOR CONTROL REGISTER 252
EXECUTION MODE WORD 253
ISOLATED SETTING 260
MASK REGISTER 262
ISOLATED MASK VALUE 263
BASE REGISTER 264
ISOLATED BASE VALUE 265
LENGTH REGISTER 266
ISOLATED LENGTH VALUE 267
OPERAND 224
270
ACCESS GENERATOR CIRCUIT
ACCESS GRANT 274
ISOLATED ACCESS 272
280
BUS CYCLE DECODER
ISOLATED ACCESS 272
ISOLATED BUS CYCLE 230
ACCESS INFORMATION 226
PHYSICAL ADDRESS 282
READ/WRITE (RD/WR#) 284
ACCESS TYPE (MEMORY/IO#) 286

FIG. 2B

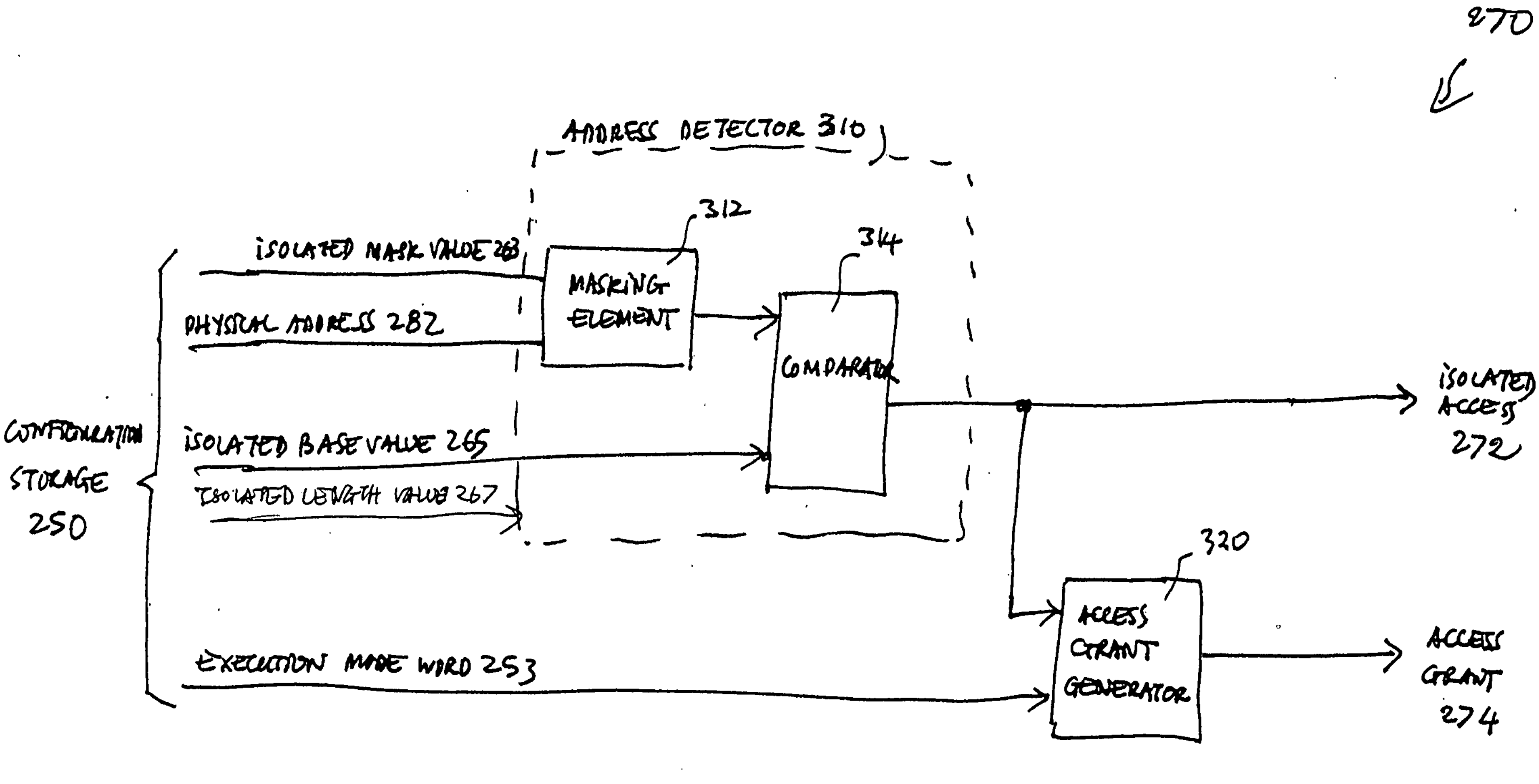
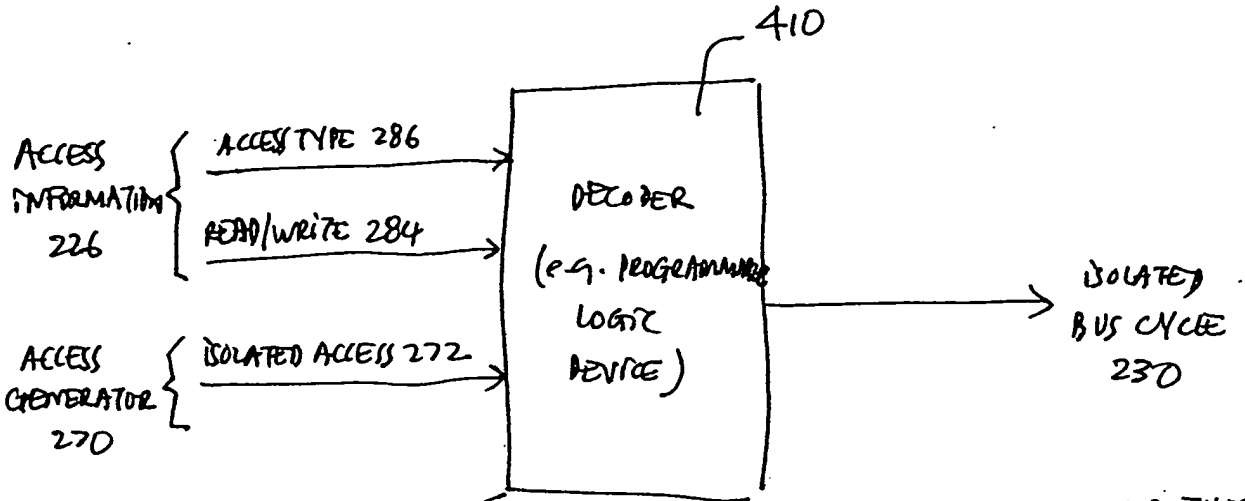


FIG. 3



TRUTH TABLE 420

ACCESS TYPE			ISOLATED ACCESS	ISOLATED BUS CYCLE		RING LEVEL
ISOLATED ENABLED STATE	M/IO#	RD/WR#				
X	X	X	DE-ASSERTED	NOT AVAILABLE		0
ENTRY (e.g., ISO_INIT)	X	X	ASSERTED	THREAT ENTRY	THREAT CYCLE	0
WITHDRAW (e.g., ISO_CLOSE)	X	X	ASSERTED	THREAT WITHDRAWAL		0
X	MEMORY REFERENCE	READ	ASSERTED	ISOLATED DATA READ	DATA ACCESS CYCLE	0
X	MEMORY REFERENCE	WRITE	ASSERTED	ISOLATED DATA WRITE		0
X	I/O REFERENCE	READ	ASSERTED	ISOLATED CONTROL READ	CONTROL ACCESS CYCLE	0
X	I/O REFERENCE	WRITE	ASSERTED	ISOLATED CONTROL WRITE		0

FIG. 4

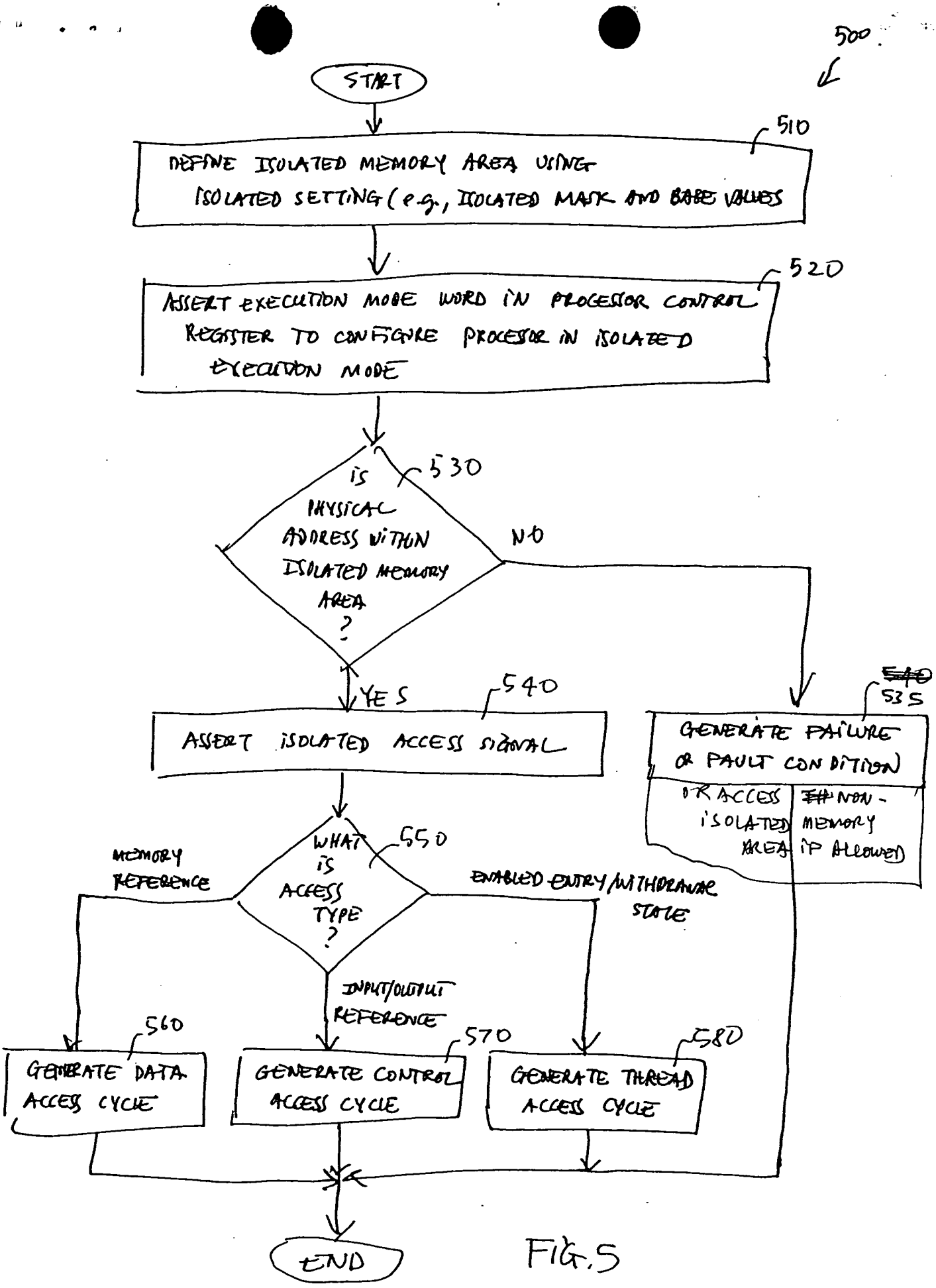

500
START
510
DEFINE ISOLATED MEMORY AREA USING ISOLATED SETTING (e.g., ISOLATED MASK AND BASE VALUES
520
ASSERT EXECUTION MODE WORD IN PROCESSOR CONTROL REGISTER TO CONFIGURE PROCESOR IN ISOLATED EXECUTION MODE
530
IS PHYSICAL ADDRESS WITHIN ISOLATED MEMORY AREA ?
NO
YES
540
ASSERT ISOLATED ACCESS SIGNAL
535
GENERATE FAILURE OR FAULT CONDITION
OR ACCESS ISOLATED MEMORY AREA IF NON-ALLOWED
550
WHAT IS ACCESS TYPE ?
MEMORY REFERENCE
INPUT/OUTPUT REFERENCE
ENABLED ENTRY/WITHDRAWAL STATE
560
GENERATE DATA ACCESS CYCLE
570
GENERATE CONTROL ACCESS CYCLE
580
GENERATE THREAD ACCESS CYCLE
END

FIG. 5